Unconditionally Secure Relativistic Quantum Bit Commitment

S.N.Molotkov and S.S.Nazin

Institute of Solid State Physics of Russian Academy of Sciences,
142432 Chernogolovka, Moscow District, Russia

Abstract

A new relativistic quantum protocol is proposed allowing to implement the bit commitment scheme. The protocol is based on the idea that in the relativistic case the field propagation to the region of space accessible to measurement requires, contrary to the non-relativistic case, a finite non-zero time which depends on the structure of the particular state of the field. In principle, the secret bit can be stored for arbitrarily long time with the probability arbitrarily close to unit.

PACS numbers: 03.65.Bz, 42.50.Dv

e-mail: molotkov@issp.ac.ru, nazin@issp.ac.ru

1 Introduction

The bit commitment scheme includes two distant users A and B and can be described as follows [1]. At the time moment t_0 user A choses one bit (0 or 1) and then sends to user B only partial information on that bit so that this information is not sufficient to find out which bit was actually chosen by user A. At the second (commitment) stage user B can ask A to send him the rest information on the bit. The protocol should provide guarantees to user B that at the second stage user A did not change his mind on the bit chosen at t_0, so that user A cannot cheat.

The classical bit commitment schemes when A and B can only exchange information through the classical channel are based on the unproven computational complexity of e.g. discrete logarithm problem. The schemes which employ a quantum information channel in addition to the classical one are called quantum bit commitment schemes. In that case information is carried by quantum states. Earlier various quantum bit commitment protocol have been proposed [2–4]. However, later the impossibility of the ideal non-relativistic quantum bit commitment protocol was proved since user A can always cheat user B by employing the EPR-pairs and delaying his measurement (actually delaying his choice of the bit) until the second stage of the protocol [5,6].

Recently, a bit commitment protocol was proposed which takes into account the finite speed of signal (information) propagation [7,8]. This relativistic classical protocol is unconditionally secure (its security is based on the fundamental laws of nature only) and allows to delay the second stage of the protocol (i.e. to store the information on the secret bit chosen by user A) for arbitrarily long time, although it requires that the two parties A and B each have a couple of spatially separated sites fully controlled by them

Below we propose a relativistic quantum protocol allowing to realize the bit commitment scheme during a finite time interval. To be more precise, in the indicated protocol the user B cannot determine the bit chosen by user A employing the information sent to him by user A during a finite time t_c (in other words, the probability of correct bit identification during arbitrarily large but finite chosen in advance time interval t_c does not exceed the probability of correct guessing of that bit, i.e. 1/2, by arbitrarily small chosen beforehand quantity ε). On the other hand, user B can ask user A at any time $t < t_c$ which bit he had actually chosen and later at any moment $T > t_c$ he can check which bit was chosen by user A at t_0. It should be noted that actually the finite time t_c is also present in the classical bit commitment protocols based on computational complexity of various problems where it is determined by the computational resources available for user B and should therefore be selected in such a way that the identification of the chosen bit from the information disclosed by user A is impossible in a time interval shorter than t_c. In our protocol the impossibility of identification of the secret bit in a time interval shorter than t_c is based on the fundamental laws of nature (like in the classical relativistic protocol [7,8]) rather than the advances in technology available for user B;

however, employment of the quantum states (to be more precise, single-particle quantum field states) as the information carriers allows to construct a protocol where each user controls a single site. In addition, in contrast to the non-relativistic quantum mechanics, the constraint on the maximum speed of information transfer allows to develop a secure protocol based on the orthogonal states.

The paper is organized as follows. Section 2 deals with quantum-mechanical measurements employed in the protocol; a simple model one-dimensional measurement is described in Section 3. The protocol itself is given in Section 4.

2 Quantum-mechanical measurements used in the protocol

All quantum cryptographic protocols actually employ the following two features of quantum theory. The first one is the no cloning theorem [16], i.e. the impossibility of copying of an arbitrary quantum state which is not known beforehand or, in other words, the impossibility of the following process:

$$|A\rangle|\psi\rangle \to U(|A\rangle|\psi\rangle) = |B_\psi\rangle|\psi\rangle|\psi\rangle,$$

where $|A\rangle$ and $|B_\psi\rangle$ are the apparatus states before and copying act, respectively, and U is a unitary operator. Such a process is prohibited by the linearity and unitary nature of quantum evolution. Actually, even a weaker process of obtaining any information about one of the two non-orthogonal states without disturbing it is impossible, i.e. the final states of the apparatus $|A_{\psi_1}\rangle$ and $|A_{\psi_2}\rangle$ corresponding to the initial input states $|\psi_1\rangle$ and $|\psi_2\rangle$, respectively, after the unitary evolution U,

$$|A\rangle|\psi_1\rangle \to U(|A\rangle|\psi_1\rangle) = |A_{\psi_1}\rangle|\psi_1\rangle,$$

$$|A\rangle|\psi_2\rangle \to U(|A\rangle|\psi_2\rangle) = |A_{\psi_2}\rangle|\psi_2\rangle,$$

can only be different, $|A_{\psi_1}\rangle \neq |A_{\psi_2}\rangle$, if $\langle\psi_1|\psi_2\rangle \neq 0$ [10], which means the impossibility of reliable distinguishing between non-orthogonal states. There is no such a restriction for orthogonal states. That is why almost all cryptographic protocols employ non-orthogonal states as information carriers, the only exception being the protocol suggested in Ref.[11].

In quantum mechanics any two orthogonal states can be reliably distinguished, and within the framework of the non-relativistic theory this can be done instantly. At the present time there is every ground to believe that in the relativistic quantum theory the orthogonal quantum states can also be reliably distinguished without disturbing them. However, the existence of a finite maximum speed of the information transfer and field propagation imposes a restriction on the time required for this process: two orthogonal states can only be reliably distinguished during a finite non-zero time interval whose duration depends on the structure of the states. The reason is that such measurements are actually non-local, as explained below.

Consider first the non-relativistic case. Suppose we are given two orthogonal states of a one-dimensional non-relativistic particle $|\psi_1\rangle$ and $|\psi_2\rangle$,

$$\langle\psi_1|\psi_2\rangle = 0. \tag{1}$$

In the momentum realization of the Hilbert space we have

$$|\psi_{1,2}\rangle = \int_{-\infty}^{\infty} \psi_{1,2}(p)|p\rangle dp. \tag{2}$$

Let the wavefunctions $|\psi_{1,2}\rangle$ have non-overlapping supports

$$\text{supp } \psi_1(p) \bigcap \text{supp } \psi_2(p) = \emptyset. \tag{3}$$

$$\langle\psi_1|\psi_2\rangle = \int_{-\infty}^{\infty} \psi_1^*(p)\psi_2(p)dp = 0.$$

The orthogonality of the states is generally a non-local property in the sense that the scalar product involves the values of the wavefunctions at all points in the space. If the states are orthogonal in the entire space, their projections on a particular subspace should not necessarily be orthogonal. To illustrate this point, consider the same states in the position realization of the Hilbert space of states:

$$|\psi_{1,2}\rangle = \int_{-\infty}^{\infty} \psi_{1,2}(x)|x\rangle dx, \quad \psi_{1,2}(x) = \int_{-\infty}^{\infty} e^{ipx}\psi_{1,2}(p)dp. \tag{4}$$

Generally, the orthogonality is only preserved in the entire space and the same states restricted to a certain subspace should not be necessarily orthogonal:

$$\langle\psi_1|\psi_2\rangle = \int_{\Omega(x)} \psi_1^*(x)\psi_2(x)dx \neq 0, \quad \text{if} \quad \Omega(x) \neq (-\infty, \infty). \tag{5}$$

Reliable distinguishing of the two states generally requires the access to the entire region of space where these states are present. Non-relativistic quantum mechanics allows instantaneous access to the entire coordinate space, that is it allows instantaneous non-local measurements. To be more precise, according to the standard non-relativistic quantum-mechanical measurement theory the outcome statistics refers to the system state at a particular moment of time. In the non-relativistic case the information on the outcome of a certain measurement involving distant points (e.g. the measuring apparatus can "read off" information on a quantum state simultaneously in different spatial points) can be gathered instantly to an observer at a certain point as long as there are no restrictions on the speed of information transfer.

Unlike the non-relativistic quantum mechanics, there is still no consistent measurement theory for the relativistic case. The instantaneous non-local measurements in the sense described above for the non-relativistic quantum mechanics seem to be impossible in the relativistic quantum theory. Even if the measuring apparatus performs simultaneous (in a certain reference frame) measurement of a quantum state in two different points $\mathbf{x}_1$ and $\mathbf{x}_2$, the information on the obtained outcomes cannot be gathered by a single localized observer in a time interval shorter than $t = |\mathbf{x}_1 - \mathbf{x}_2|/2c$. Therefore, non-local measurements require finite time which depends on the structure of the measured states.

Thus, in the relativistic quantum field theory gathering information on the outcome of a non-local measurement requires a finite time. In addition, if the measuring apparatus has only access to a limited domain D of space, the measurement performed over a non-stationary state would only provide information on that state if its spatial supports has common points with D at the time of measurement. If the state support lies outside D at time t_0, the full information on the state employing the measurements restricted to D is only possible in time $t_1 \approx L/2c$, where L is the size of the state support since the state cannot move into the domain D in less than t_1 because of the constraint on the maximum field propagation speed.

Before describing the protocol, we shall first discuss the measurements it employs. In the rest of the paper we shall deal with the massless particles (photons). The four-dimensional vector-potential operators have the form [12]

$$A_n^{\pm}(\hat{x}) = \frac{1}{(2\pi)^{3/2}} \int e^{\pm i\hat{k}\hat{x}} A_n^{\pm}(\mathbf{k}) \frac{d\mathbf{k}}{\sqrt{2k^0}} = \frac{1}{(2\pi)^{3/2}} \int e^{\pm i\hat{k}\hat{x}} e_n^m(\mathbf{k}) a_m^{\pm}(\mathbf{k}) \frac{d\mathbf{k}}{\sqrt{2k^0}}, \tag{6}$$

where $\hat{k}\hat{x} = k^0x^0 - \mathbf{kx}$. The operators $A_n^{\pm}(\hat{x})$ are supposed to satisfy the Bose commutation relations [12]

$$[A_m^-(\hat{x}_1), A_n^+(\hat{x}_2)]_- = ig_{mn}D_0^-(\hat{x}_1 - \hat{x}_2), \tag{7}$$

where g^{nm} is the metric tensor ($g^{00} = -g^{11} = -g^{22} = -g^{33} = 1$), D_0^- is the negative-frequency commutator function for the massless field

$$D_0^-(\hat{x}) = -i\frac{1}{(2\pi)^{3/2}} \int d\hat{k}\delta(\hat{k}^2)\theta(-k^0)e^{i\hat{k}\hat{x}} = \frac{i}{(2\pi)^3} \int \frac{d\mathbf{k}}{2|\mathbf{k}|} e^{-ix^0|\mathbf{k}|+i\mathbf{xk}}, \tag{8}$$

which is only different from zero and has a singularity on the light cone [12]

$$D_0^-(\hat{x}) = \frac{1}{4\pi}\varepsilon(x^0)\delta(\lambda), \quad \lambda^2 = (x^0)^2 - \mathbf{x}^2. \tag{9}$$

Further we put $c = 1$. The creation and annihilation operators $a_m^{\pm}(\mathbf{k})$ describe the photons of four types: two transverse, one longitudinal, and one temporal. The two latter types are non-physical and are only introduced to preserve the four-dimensional structure of the vector-potential. The commutation relations are

$$[a_m^-(\mathbf{k}), a_n^+(\mathbf{k}')]_- = -g^{nm}\delta(\mathbf{k}-\mathbf{k}'), \quad (\mathbf{e}^\alpha\cdot\mathbf{e}^\beta) = \delta_{\alpha,\beta}, \quad (\alpha,\beta = 1,2,3), \quad e_0^\alpha = 0, \quad \mathbf{e}^3 = \frac{\mathbf{k}}{|\mathbf{k}|}.$$

When working with the four types of photons one should employ the indefinite metric. For our purposes it is sufficient to deal with a single sort of photons with a fixed helicity and we shall therefore work in the subspace of one-particle states equipped with a standard hermitian scalar product (for details see Ref.[12]).

The one-photon states corresponding to the bit values 0 and 1, respectively, $|\psi_1\rangle$ and $|\psi_2\rangle$, can be chosen in the form

$$|\psi_{1,2}\rangle = \int \psi_{1,2}(\mathbf{k}) a^+(\mathbf{k},s)|0\rangle \frac{d\mathbf{k}}{\sqrt{2k^0}} = \int \psi_{1,2}(\mathbf{k})|\mathbf{k},s\rangle \frac{d\mathbf{k}}{\sqrt{2k^0}}, \quad \langle \mathbf{k},s|\mathbf{k}',s\rangle = \delta(\mathbf{k}-\mathbf{k}'), \tag{10}$$

where $a^+(\mathbf{k},s)$ is the operator of creation of a photon with momentum $\mathbf{k}$ and helicity s. We assume that the state amplitudes have non-overlapping supports

$$\text{supp } \psi_1(\mathbf{k}) \bigcap \text{supp } \psi_2(\mathbf{k}) = \emptyset, \quad \Omega_i(\mathbf{k}) = \text{supp } \psi_i(\mathbf{k}). \tag{11}$$

Then the states $|\psi_1\rangle$ and $|\psi_2\rangle$ are orthogonal

$$\langle\psi_1|\psi_2\rangle = \int \psi_1^*(\mathbf{k})\psi_2(\mathbf{k})\frac{d\mathbf{k}}{2k^0} = 0. \tag{12}$$

The measurement allowing to reliably distinguish between the two orthogonal states $|\psi_1\rangle$ and $|\psi_2\rangle$ is given by the identity resolution

$$\mathcal{P}_{\psi_1} + \mathcal{P}_{\psi_2} + \mathcal{P}_\perp = I, \quad I = \int |\mathbf{k},s\rangle\langle\mathbf{k},s|\frac{d\mathbf{k}}{2k^0}, \tag{13}$$

$$\mathcal{P}_{\psi_{1,2}} = \left(\int_{\Omega_{1,2}(\mathbf{k})} \psi_{1,2}(\mathbf{k})|\mathbf{k},s\rangle \frac{d\mathbf{k}}{\sqrt{2k^0}}\right)\left(\int_{\Omega_{1,2}(\mathbf{k})} \langle\mathbf{k}',s|\psi_{1,2}^*(\mathbf{k}')\frac{d\mathbf{k}'}{\sqrt{2k^{0'}}}\right), \quad \mathcal{P}_\perp = I - \mathcal{P}_{\psi_1} - \mathcal{P}_{\psi_2}.$$

The probabilities of different outcomes for the input state $|\psi_1\rangle$ are given by the relations

$$\Pr_1\{\mathcal{P}_{\psi_1}\} = \mathrm{Tr}\{|\psi_1\rangle\langle\psi_1|\mathcal{P}_{\psi_1}\} = \left(\int_{\Omega_1(\mathbf{k})} |\psi_1(\mathbf{k})|^2 \frac{d\mathbf{k}}{2k^0}\right)\left(\int_{\Omega_1(\mathbf{k}')} |\psi_1(\mathbf{k}')|^2 \frac{d\mathbf{k}'}{2k^{0'}}\right) \equiv 1, \tag{14}$$

$$\Pr_{\psi_1}\{\mathcal{P}_{\psi_2,\perp}\} = \mathrm{Tr}\{|\psi_1\rangle\langle\psi_1|\mathcal{P}_{\psi_2,\perp}\} \equiv 0,$$

and similarly for the input state $|\psi_2\rangle$.

To illustrate the non-local nature of the measurement (13) more clearly, let us consider an auxiliary measurement in the position representation which transforms to the measurement allowing reliable distinguishing of the two states when the involved spatial domain is extended to the entire space.

Consider first an auxiliary measurement which allows to reliably distinguish between any two states with non-overlapping supports rather than a particular pair of states. This measurement is very similar to the measurement (13):

$$\mathcal{P}_1 + \mathcal{P}_2 + \mathcal{P}_\perp = I, \quad I = \int |\mathbf{k},s\rangle\langle\mathbf{k},s|\frac{d\mathbf{k}}{2k^0}, \tag{15}$$

$$\mathcal{P}_{1,2} = \int_{\Omega_{1,2}(\mathbf{k})} |\mathbf{k}, s\rangle\langle\mathbf{k}, s|\frac{d\mathbf{k}}{2k^0}, \quad \mathcal{P}_{\perp} = I - \mathcal{P}_1 - \mathcal{P}_2.$$

The probabilities of different outcomes for the input state $|\psi_1\rangle$ are

$$\mathrm{Pr}_1\{\mathcal{P}_1\} = \mathrm{Tr}\{|\psi_1\rangle\langle\psi_1|\mathcal{P}_1\} = \int_{\Omega_1(\mathbf{k})} |\psi_1(\mathbf{k})|^2 \frac{d\mathbf{k}}{2k^0} \equiv 1, \tag{16}$$

$$\mathrm{Pr}_1\{\mathcal{P}_{2,\perp}\} = \mathrm{Tr}\{|\psi_1\rangle\langle\psi_1|\mathcal{P}_{2,\perp}\} \equiv 0,$$

and similarly for the input state $|\psi_2\rangle$.

According to the quantum-mechanical measurement theory, any measurement is described by the positive identity resolution on the Hilbert space of the system states, or, to be more precise, by the positive operator-valued measure M (on a certain measurable outcome space $\mathcal{U}$) satisfying the conditions [13]

$$\begin{aligned} &1) \quad M(\emptyset) = 0, \quad M(\mathcal{U}) = I, \quad M(\mathcal{U}_i) \geq 0, \\ &2) \quad M(\mathcal{U}_1) \leq M(\mathcal{U}_2), \quad \mathcal{U}_1 \subseteq \mathcal{U}_2, \\ &3) \quad M(\bigcup_i \mathcal{U}_i) = \Sigma_i M(\mathcal{U}_i), \quad \mathcal{U}_i \bigcap \mathcal{U}_j = \emptyset. \end{aligned} \tag{17}$$

We shall choose a three-element discrete space whose points are labeled by the symbols $\{1, 2, \perp\}$ as the space of outcomes:

$$M_{1,2} = \int_{\Omega(\mathbf{x})} d\mathbf{x} \left(\int_{\Omega_{1,2}(\mathbf{k})} e^{i\hat{k}(\hat{x}-\hat{x}_0)} |\mathbf{k}, s\rangle \frac{d\mathbf{k}}{\sqrt{2k^0}} \right) \left(\int_{\Omega_{1,2}(\mathbf{k}')} e^{-i\hat{k}'(\hat{x}-\hat{x}_0)} \langle\mathbf{k}', s| \frac{d\mathbf{k}'}{\sqrt{2k^{0'}}} \right), \tag{18}$$

$$M_{\perp} = \int_{\mathcal{X}} \int_{\mathcal{K}} \int_{\mathcal{K}} d\mathbf{x} \left(e^{i\hat{k}(\hat{x}-\hat{x}_0)} |\mathbf{k}, s\rangle \frac{d\mathbf{k}}{\sqrt{2k^0}} \right) \left(e^{-i\hat{k}'(\hat{x}-\hat{x}_0)} \langle\mathbf{k}', s| \frac{d\mathbf{k}'}{\sqrt{2k^{0'}}} \right) - M_1 - M_2, \tag{19}$$

where

$$\mathcal{X} = \{\mathbf{x} : \quad \mathbf{x} \in (-\infty, \infty)\},$$
$$\mathcal{K} = \{\mathbf{k} : \quad \mathbf{k} \in (-\infty, \infty)\}.$$

The positive operator-valued measure M_i defines an identity resolution on the space of outcomes $\{1, 2, \perp\}$:

$$M_1 + M_2 + M_{\perp} = \int_{\mathcal{X}} \int_{\mathcal{K}} \int_{\mathcal{K}} d\mathbf{x} \left(e^{i\hat{k}(\hat{x}-\hat{x}_0)} |\mathbf{k}, s\rangle \frac{d\mathbf{k}}{\sqrt{2k^0}} \right) \left(e^{-i\hat{k}'(\hat{x}-\hat{x}_0)} \langle\mathbf{k}', s| \frac{d\mathbf{k}'}{\sqrt{2k^{0'}}} \right) = \tag{20}$$

$$= \int_{\mathcal{K}} |\mathbf{k}, s\rangle\langle\mathbf{k}, s| \frac{d\mathbf{k}}{2k^0} = I.$$

First of all, it is seen from (19,20) that when the spatial domain $\Omega(\mathbf{x})$ is extended to the entire position space $\mathcal{X}$ the measurement transforms to the orthogonal identity resolution (15) which allows to reliably distinguish between the states with non-overlapping supports.

For example, the probability of obtaining the outcome 1 for the input state $|\psi_1\rangle$ is

$$\mathrm{Pr}_1\{M_1\} = \mathrm{Tr}\{|\psi_1\rangle\langle\psi_1|M_1\} =$$

$$\int_{\Omega(\mathbf{x})} d\mathbf{x} \left(\int_{\Omega_1(\mathbf{k})} e^{i\hat{k}(\hat{x}-\hat{x}_0)} \psi_1^*(\mathbf{k}) \frac{d\mathbf{k}}{2k^0} \right) \left(\int_{\Omega_1(\mathbf{k})} e^{-i\hat{k}'(\hat{x}-\hat{x}_0)} \psi_1(\mathbf{k}') \frac{d\mathbf{k}'}{2k^{0'}} \right) = \tag{21}$$

$$= -(2\pi)^6 \int_{\Omega(\mathbf{x})} d\mathbf{x} \mid \psi_1(-i\frac{\partial}{\partial \mathbf{x}}) \mid^2 D_0^-(\hat{x} - \hat{x}_0) D_0^+(\hat{x}_0 - \hat{x}).$$

Since the amplitude $\psi_1(\mathbf{k})$ has a finite support, i.e. it vanishes outside the domain $\Omega_1(\mathbf{k})$, the domain of integration over $\mathbf{k}, \mathbf{k}'$ in Eq.(21) can be extended to the entire space $\mathcal{K}$. We assume the amplitude

$\psi_1(\mathbf{k})$ to be a sufficiently smooth function to allow the substitution of the argument $\mathbf{k}$ by $i\partial/\partial\mathbf{x}$ followed by its extraction outside the integral sign over $\mathbf{k}$. Further, taking into account the definition of function $D_0^-(\hat{x})$ (8), one obtains the final expression. Remember also that $D_0^-(\hat{x}) = -D_0^+(\hat{-x})$. The probability of obtaining outcome 2 for the input state $|\psi_1\rangle$ is identically equal to zero (and similarly for the outcome 2 with the input state $|\psi_2\rangle$):

$$\mathrm{Pr}_1\{M_2\} = \mathrm{Tr}\{|\psi_1\rangle\langle\psi_1|M_2\} = \tag{22}$$

$$\int_{\Omega(\mathbf{x})} d\mathbf{x} \left(\int_{\Omega_2(\mathbf{k})} e^{i\hat{k}(\hat{x}-\hat{x}_0)} \psi_1^*(\mathbf{k}) \frac{d\mathbf{k}}{2k^0} \right) \left(\int_{\Omega_2(\mathbf{k})} e^{-i\hat{k}'(\hat{x}-\hat{x}_0)} \psi_1(\mathbf{k}') \frac{d\mathbf{k}'}{2k^{0'}} \right) \equiv 0,$$

since the amplitudes $\psi_1(\mathbf{k})$ and $\psi_2(\mathbf{k})$ possess non-overlapping supports.

Finally, the probability of obtaining the outcome $\perp$ for the input state $|\psi_1\rangle$ (and, similarly, for $|\psi_2\rangle$) is

$$\mathrm{Pr}_1\{M_\perp\} = \mathrm{Tr}\{|\psi_1\rangle\langle\psi_1|M_\perp\} =$$

$$\int_{\mathcal{X}\setminus\Omega(\mathbf{x})} d\mathbf{x} \left(\int_{\Omega_1(\mathbf{k})} e^{i\hat{k}(\hat{x}-\hat{x}_0)} \psi_1^*(\mathbf{k}) \frac{d\mathbf{k}}{2k^0} \right) \left(\int_{\Omega_1(\mathbf{k})} e^{-i\hat{k}'(\hat{x}-\hat{x}_0)} \psi_1(\mathbf{k}') \frac{d\mathbf{k}'}{2k^{0'}} \right) = \tag{23}$$

$$= -(2\pi)^6 \int_{\mathcal{X}\setminus\Omega(\mathbf{x})} d\mathbf{x} \mid \psi_1(-i\frac{\partial}{\partial\mathbf{x}}) \mid^2 D_0^-(\hat{x}-\hat{x}_0) D_0^+(\hat{x}_0-\hat{x}).$$

The measurement (19–23) has a simple meaning. The equation (21) describes the probability of detection in the spatial domain $\Omega(\mathbf{x})$ of the state whose support lies in $\Omega_1(\mathbf{k})$ (and similarly for $|\psi_2\rangle$).

Reliable detection of the states whose support lies in $\Omega_1(\mathbf{k})$ requires the access to the entire spatial domain where the state is present; it is seen from Eq.(21) that contribution to the probability is only given by the causally related points ($(\hat{x}-\hat{x}_0)^2 = 0$, $|\mathbf{x_0}-\mathbf{x}| = c|t_0 - t|$) since the commutator functions $D_0^{\pm}(\hat{x}-\hat{x}_0)$ are only different from zero on the light cone. In spite of the fact that the commutation functions in (21,22) both have a singularity on the light cone, their product always exists as a distribution since the Fourier transforms of D^--functions have their supports in the front part of the light cone (for details see e.g. [14]).

Equation (23) yields the probability of detection of a state with the support in $\Omega_1(\mathbf{k})$ (and similarly for $|\psi_2\rangle$) in the rest part of the space $\mathcal{X}\setminus\Omega(\mathbf{x})$ due to the "tails" of the state $|\psi_1\rangle$ which do not "fit" into the spatial domain $\Omega(\mathbf{x})$. When the accessible domain $\Omega(\mathbf{x})$ is extended to the extent that the entire state $|\psi_1\rangle$ can "fit" into it, the measurement discussed transforms to the measurement corresponding to the orthogonal projectors (15) which allows to reliably (with unit probability) distinguish between the two states, the probability of detection of the "tails" $\perp$ tending to zero.

Eq.(21) is especially transparent for the state which is strongly localized in the position space. In that case the state amplitude in the momentum space is strongly delocalized (in the limit $|\psi_1(\mathbf{k})|^2) \to$ const the support $\Omega_1(\mathbf{k}) \to \mathcal{K}$ and, accordingly, $|\psi(-i\partial/\partial\mathbf{x})|^2$ does not depend on $\mathbf{x}$). Eq. (21) becomes

$$\mathrm{Pr}_1\{M_1\} = (2\pi)^6 \int_{\Omega(\mathbf{x})} d\mathbf{x} \mid D_0^-(\hat{x}-\hat{x}_0) \mid^2 . \tag{24}$$

If we now remember that the function $-iD_0^-(\hat{x}-\hat{x}_0)$ describes the amplitude of the propagation of a one-particle field state created at a point $\hat{x}_0$ to the point $\hat{x}$

$$\langle 0|\psi_1^-(\hat{x})\psi_1^+(\hat{x}_0)|0\rangle = -iD_0^-(\hat{x}-\hat{x}_0), \quad x_0 > x_0^0, \tag{25}$$

then Eq.(21) yields the probability of detection of the one-particle field state with the support in $\Omega_1(\mathbf{k}) \to \mathcal{K}$ in the spatial domain $\Omega(\mathbf{x})$. It is seen from Eq.(24), that if the integration domain $\Omega(\mathbf{x})$ does not include the points where the one-particle state was created $\hat{x}_0$ the detection probability is zero. For reliable detection of a strongly spatially localized state the spatial domain should be chosen arbitrarily small, $\Omega(\mathbf{x}) \to 0$. The field can "fill in" this domain arbitrarily fast (naturally, excluding the time-of-flight from the creation point $\hat{x}_0$ to $\Omega(\mathbf{x})$).

On the contrary, if the state is not strongly localized in space (so that $|\psi_1(\mathbf{k})|^2 \neq const$ and, accordingly, $|\psi_1(-i\partial/\partial\mathbf{x})|^2 \neq const$), the contributions are given by all the points of the domain $\Omega(\mathbf{x})$. The stronger the state is localized in the $\mathbf{k}$-space, the stronger it is delocalized in the position space and the larger domain $\Omega(\mathbf{x})$ is required for a reliable (with unit probability) detection of the state. The field cannot "fill in" that domain in time less than $t \approx L(\Omega(\mathbf{x}))/c$, where L is the characteristic domain size.

It will be important for the bit commitment protocol that the detection probability grows with time (as the field fills the domain accessible to the measurement) and finally after the time T elapses (this time depends on the structure of the particular state) the states become reliably distinguishable due to their orthogonality. During the time interval $0 < t < T$ the states are effectively non-orthogonal (non-distinguishable reliably). Choosing the supports $\Omega_{1,2}(\mathbf{k})$ of the states more and localized the time interval T can be made arbitrarily long.

Because of the symmetry between 0 and 1 it is convenient to choose the states in such a way that the domain $\Omega(\mathbf{x})$ be the same for them (the correct identification probabilities as functions of time will then be identical for 0 and 1). For the photons this can always be done by choosing, for example, a pair of narrow-band state with the same frequency width and different central frequencies.

It should be emphasized that Eqs.(21–23) are statistical in nature. If the domain accessible in the measurement procedure is small, or equivalently, the state should be identified in a short time, the probability of the correct answer is small, since most of the outcomes will occur in the channel $M_\perp$ independently of the income state. The probabilities of the outcomes 1 and 2 are small due to the smallness of the domain accessible to the detection procedure. However, firing of the detector in the channel M_1 or M_2 is sufficient to correctly identify the state, the problem being the low probability of the corresponding events.

It is also easy to write down the measurement involving a finite spatial domain and allowing to reliably distinguish between a pair of particular orthogonal states $|\psi_1\rangle$ and $|\psi_2\rangle$ (rather than the states with non-overlapping supports) when the spatial domain $\Omega(\mathbf{x})$ is extended to the entire position space:

$$M_{1,2} = \tag{26}$$

$$\left(\int_{\Omega(\mathbf{x})} d\mathbf{x} \int_{\mathcal{K}}\int_{\mathcal{K}} \psi_{1,2}(\mathbf{k}) e^{i(\hat{k}-\hat{k}')(\hat{x}-\hat{x}_0)} |\mathbf{k}\rangle \frac{d\mathbf{k}d\mathbf{k}'}{(2k^0 2k^{0\prime})^{1/4}}\right)\left(\int_{\Omega(\mathbf{x})} d\mathbf{x} \int_{\mathcal{K}}\int_{\mathcal{K}} \langle\mathbf{k}|\psi^*_{1,2}(\mathbf{k}) e^{-i(\hat{k}-\hat{k}')(\hat{x}-\hat{x}_0)} \frac{d\mathbf{k}d\mathbf{k}'}{(2k^0 2k^{0\prime})^{1/4}}\right),$$

$$M_\perp = I - M_1 - M_2. \tag{27}$$

When the accessible domain is extended to the entire space ($\Omega(\mathbf{x}) \to \mathcal{X}$) this measurements transforms to the orthogonal projectors given by Eq.(13).

3 Example of a one-dimensional measurement

To get a qualitative picture and obtain more accurate estimates, we shall consider a model one-dimensional situation since the three-dimensional case requires the specification of the geometry of spatial domains. In addition, the experimental realization usually employ the optical fiber (which is a one-dimensional system) as the quantum channel. Similar model one-dimensional schemes are frequently used in quantum optics.

Suppose we have a pair of orthogonal single-photon packets

$$|\psi_{1,2}\rangle = \int_0^\infty \psi_{1,2}(k)|k\rangle dk, \quad \rho_{1,2} = |\psi_{1,2}\rangle\langle\psi_{1,2}|, \quad k > 0, \quad \langle k|k'\rangle = \delta(k-k'), \tag{28}$$

where $|k\rangle = a^+_k|0\rangle$ is the single-photon monochromatic Fock state (we consider the particles moving in only one direction). In addition, in the one-dimensional case, $k^0 = k$ ($c = 1$ is the velocity of light).

The states have non-overlapping supports with the same bandwidth

$$E_{1,2} = \mathrm{supp}\ \psi_{1,2} = \{k : \quad k \in (-\Delta/2 + k_{1,2}, k_{1,2} + \Delta/2)\}, \quad E = \{k : \quad k \in [0, \infty)\}, \tag{29}$$

$$k_1 - k_2 \geq \Delta, \quad \int_{E_{1,2}} |\psi_{1,2}(k)|^2 dk = 1,$$

The states with the non-overlapping supports are orthogonal

$$\langle\psi_1|\psi_2\rangle = \int_0^\infty \psi_1^*(k)\psi_2(k)dk = 0. \tag{30}$$

The measurement allowing to reliably distinguish between the states (28) is given by the identity resolution similar to Eq.(15)

$$\mathcal{P}_1 + \mathcal{P}_2 + \mathcal{P}_\perp = I, \quad I = \int_0^\infty |k\rangle\langle k|dk, \quad \mathcal{P}_{1,2} = \int_{E_{1,2}} |k\rangle\langle k|dk, \quad \mathcal{P}_\perp = \int_{E\setminus(E_1\bigcup E_2)} |k\rangle\langle k|dk. \tag{31}$$

The identity resolution (31) does not involve the position and time parameter indicating that it is implicitly assumed that the spatial domain accessible to the measurement procedure is $x \in (-\infty, \infty)$.

In the one-dimensional case the measurement M_i similar to (19,20) has the same form, the only difference being the replacement of the three-dimensional domain $\Omega(\mathbf{x})$ by the one-dimensional which for brevity will be denoted as $\mathcal{X} = \{x : \quad x \in (-X, X)\}$. The one-dimensional case is especially transparent, since the time parameter and position appear in the combination $x - ct$ which is actually related to the properties of the fundamental solution of the one-dimensional wave equation which is known to have the form $\mathcal{E}(x,t) =\propto \theta(ct - |x|)$ unlike the three-dimensional case ($\mathcal{E}(x,t) \propto \theta(t)\delta(c^2t^2 - |\mathbf{x}|^2)$) [15]. Therefore, in the one-dimensional case expansion of the spatial domain X accessible in the measurement can be effectively obtained (for fixed X) by increasing the accessible time interval T. Taking the above consideration in the account we shall below speak for brevity that the measurements are performed in the accessible time window $(-T, T)$.

The probability of occurrence of the outcome 1 for the input density matrix ρ_1 in the one-dimensional case is conveniently written (first performing integration over x) as

$$\Pr{}_1\{M_1\} = \mathrm{Tr}\{\rho_1 M_1\} = \int_{E_1}\int_{E_1} \psi_1^*(k)\psi_1(k')\frac{\sin[(k-k')T]}{(k-k')}dkdk', \quad T \equiv ct - |X|. \tag{32}$$

Eq.(32) yields the probability of detection of the systems whose density matrix has the support in E_1 during the time window $(-T, T)$.

If the time window during which the measurements are allowed is short ($T\Delta \ll 1$), Eq.(32) yields

$$\Pr{}_1\{\ M_1\} \approx T\Delta \ll 1 \approx 0, \tag{33}$$

i.e. the detection probability is proportional to the time window duration. For a long time window ($T\Delta \gg 1$) one has

$$\Pr{}_1\{\ M_1\} \approx \frac{1}{\pi}\int_{-T}^{T} \frac{\sin\xi}{\xi}d\xi = 1 - \cos(T\Delta)/T\Delta \approx 1, \quad T\Delta \gg 1. \tag{34}$$

If the input state is ρ_2, the probability of obtaining outcome 2 is zero independently of the time window duration T (and similarly for ρ_1 and outcome 2):

$$\Pr{}_2\{M_1\} = \mathrm{Tr}\{\rho_2 M_1\} = \Pr{}_1\{M_2\} = \mathrm{Tr}\{\rho_1 M_2\} = 0. \tag{35}$$

Eq.(32) can be rewritten in a more usual form as

$$\Pr{}_1\{M_1\} = \int_{-T}^{T} |\psi_1(\tau)|^2 d\tau, \quad \psi_1(\tau) = \int_0^\infty \psi_1(k)e^{-ik\tau}dk, \tag{36}$$

which is consistent with the intuitive classical concepts. If the function is localized in the frequency representation, it is delocalized in the temporal representation, so that reliable signal detection requires a long time window which can fully "cover" $\psi(\tau)$.

Here one reservation is in place. If we are given a classical state, i.e. a classical function $\psi(x)$ with the beforehand unknown support in the k-representation (supp $\psi(k) = \Delta$), the support can only be found if one finds the values of the function in the spatial domain whose size is not less than $L_x \approx 1/\Delta$. On the other hand, if one has to distinguish between the two classical functions $\psi_1(k)$ and $\psi_2(k)$ with non-overlapping supports it is sufficient to know the function values in a single point x where $\psi_1(x) \neq \psi_2(x)$. Therefore, reliable distinguishing between the two classical functions requires the knowledge of the function values in a single point where these values are different.

To reliably distinguish between the two orthogonal quantum states $|\psi_1\rangle$ and $|\psi_2\rangle$ with unit probability one requires the access to the entire spatial domain where these states are different from zero (we assume that both states are different from zero in the same domain).

For a short time window ($T \ll 1/\Delta$, where Δ is the bandwidth) the detection probability is small to the extent $T\Delta \ll 1$. If the detection occurs in channels 1 or 2, this is sufficient to reliably distinguish between the states $|\psi_1\rangle$ and $|\psi_2\rangle$. However, for a short time window dominating for both input states $|\psi_1\rangle$ and $|\psi_2\rangle$ will be the detection events in channel $\perp$, i.e. the states will be indistinguishable with the probability close to 1 (effectively non-orthogonal).

The outcomes in channel $\perp$ will occur in the time window $(-\infty, \infty)$ due to the states whose supports do not lie in E_1 or E_2 and, in addition, in the time intervals $(-\infty, -T)$ and (T, ∞) due to the "tails" of the states with the supports in $E_{1,2}$ which were not detected in the channels $1, 2$ in the time window $(-T, T)$.

The detection probability of $\rho_{1,2}$ in the channel $\perp$ is

$$\Pr_{1,2}\{\perp\} = \int_{E_{1,2}} \int_{E_{1,2}} \left\{ \delta(k-k') - \frac{\sin[(k-k')T]}{(k-k')} \right\} \psi^*_{1,2}(k)\psi_{1,2}(k')dkdk'. \quad (37)$$

For $T\Delta \gg 1$ (long time window) we have

$$\Pr_{1,2}\{\perp\} \approx \cos(T\Delta)/T\Delta \to 0, \quad (38)$$

while for $T\Delta \ll 1$ (short time window)

$$\Pr_{1,2}\{\perp\} \approx \sin(T\Delta)/T\Delta \to 1. \quad (39)$$

Eqs.(32–39) actually mean that if one of the states ρ_1 or ρ_2 is given and one should identify which state is actually given during the time interval T then for $T \ll 1/\Delta$ the probability of the correct identification $p_+ \approx T\Delta \ll 1$ (accordingly, the wrong answer probability is $p_- \approx 1 - T\Delta \sim 1$), since the detection probability in the time interval T is small. On the other hand if the measurements are allowed to be performed in th long time window ($T\Delta \gg 1$), the probability of the correct answer $p_+ \approx 1 - 1/T\Delta \approx 1$ so that the states are reliably distinguishable.

For a short time window the sates are effectively non-orthogonal (they cannot be distinguished reliably). The effective angle α between the states ρ_1 and ρ_2 in the time interval $(-T, T)$ is small

$$\langle\psi_1|\psi_2\rangle \approx \cos\alpha \approx 1 - T\Delta, \quad \alpha \approx T\Delta \ll 1. \quad (40)$$

4 Relativistic quantum bit commitment protocol

Let us now describe the bit commitment protocol. The two parties agree in advance on the states $|\psi_1\rangle$ and $|\psi_2\rangle$ corresponding to 0 and 1 as well as on the number N of quantum systems sent by user A to B. It is always possible to choose a pair of orthogonal states so that their spatial extent strongly exceeds the channel length and their fall-off at the infinity insures almost reliable identification after the time T elapses. In the case of photons one can choose two states with sufficiently narrow energy spectra so that their effective extent $L \approx c/\Delta\omega$ ($\Delta\omega$ is the energy spectrum width) substantially exceeds the communication channel length L_{ch}, In that case the channel length can effectively assumed to be zero. Formally that means that the two parties A and B can only control the neighbourhoods of the points

x_A and x_B and do not control the space outside these neighbourhoods. In other words, outside the neighbourhoods of x_A and x_B both parties are allowed to do anything which does not contradict the laws of relativistic quantum mechanics.

The user A chooses his bit a (0 or 1), which is the parity bit of N quantum states ($a = a_1 \oplus a_2 \oplus \ldots \oplus a_N$). Then at time $t = 0$ the user A sends to B all N states simultaneously. To be more precise, user A turns on N sources producing the states which are allowed to propagate into the communication channel as long as they are being formed. Since the states $|\psi_1\rangle$ and $|\psi_2\rangle$ are generally non-stationary, fixing the time moment $t = 0$ allows user B to "tune" the measurement (13) by choosing appropriate phase shifts for any spatial domain reached by the field as it is propagating in the communication channel. User B performs measurements (13) separately on each state. Because of the orthogonality, the states become distinguishable by the time T when they are first fully accessible. In the time interval $0 < t < T$ the states are not fully accessible (effectively non-orthogonal) and therefore are not reliably distinguishable. The probability of correct identification of the states is an increasing function of time ($p(t = 0) = 0$ and $p(t = T) = 1$), the specific form of $p(t)$ depending on the structure of the particular states used and being irrelevant for our analysis. For individual measurements the probability of the correct identification of the parity bit $P_+(t) = p^N(t) \ll 1$ as long as $p(t) \ll 1$. For collective measurements, when the measurements are performed over all N states as a whole the probability of the correct parity bit identification is $P_+^{collect}(t) = \sqrt{p^N(t)} \ll 1$ [16] and can also be made arbitrarily small by appropriate choice of the states used. The states can always be chosen in such a way that for an arbitrarily small quantity $\delta \ll 1$ specified beforehand and arbitrarily large time t_c (t_c is the time of secure storage of the secret bit chosen by user A) the probability $P_+^{collect}(t)$ of the correct identification of the parity bit during time $t < t_c$ is arbitrarily small. This can be achieved by increasing the effective extent of the states (reducing the spectrum width).

The above discussion concerns the case where the user B obtains the information on the states only from the quantum-mechanical measurements. The mentioned probabilities $p(t)$ actually represent the probabilities of the state detection (firing of a classical apparatus) which for times $t < T$ is less than 1 because the entire state is not accessible for the measurement. However, if the detection did take place, the state can be identified by the obtained measurement outcome. Therefore, as long as the probability of the detection itself $p_i(t) < 1/2$, the user B can even perform no measurements simply guessing the states sent in each communication channel. However, for the times when $p_i(t) > 1/2$ the measurements provide more information than simple guessing without performing any measurements. For $t \to T$ the measurements provide almost reliable information on the states.

Therefor, the probability $P^{store}(t)$ of secure storage of the secrete bit chosen by user A is a decreasing function of time ($P^{store}(t = 0) = 1$ and $P^{store}(t = T) = 0$).

After the quantum part of the protocol is completed at $t > T$, when user B already has the full access to the states and can reliably identify them, user A discloses through a classical channel which states he sent through each of N quantum channels. Any inconsistency between the classical information and the measurement result in at least one channel aborts the protocol. The necessity of conveying the classical information by user A after the quantum-mechanical measurements and the individual reliable distinguishability (orthogonality) of the states eliminates the possibility of cheating. For example, user A cannot send the mixed states like $\rho = |\psi_1\rangle\langle\psi_1| + |\psi_2\rangle\langle\psi_2|$, since for large N this would result in the discrepancy between the classical information and the outcomes of quantum measurements. Neither can he send any other states instead of $|\psi_1\rangle$ and $|\psi_2\rangle$ because of their orthogonality, i.e. reliable distinguishability. Any different states would yield for large N wrong outcomes if the measurement $\mathcal{P}_{1,2,\perp}$ is used. The constraints on the maximum field state propagation velocity does not allow the user A to delay sending his states to user B since the measurement (13) is "tuned" to precisely the states $|\psi_1\rangle$ and $|\psi_2\rangle$ so that the delayed states would produce wrong outcomes. Formally, the delay can be described as a translation in the space-time which results in an additional phase factor $e^{i\hat{k}\hat{x}_0}$ under the integral sign in (10). The "shifted" state, e.g. $|\psi_1\rangle$, will not yield the outcome 1 with the unit probability.

In the non-relativistic case the user A can employ the EPR pair which allows him to delay his choice of the secret bit until the measurement performed by user B [5,6]. In the relativistic case the EPR-attack does not work because of the constraint on the maximum speed of the field state propagation. In spite of the fact that the EPR correlations are also preserved in the relativistic case for the measurements performed on the entangled two-particle states of the field at the points separated by the space-like interval [17], the field cannot propagate from the EPR-source faster than light. Therefore, in contrast to the non-relativistic quantum mechanics, employment by user A of an EPR-pair to delay his choice until the second stage of the protocol does not work.

It should be noted once again that it is important for the protocol that the orthogonal states have quantum nature, so that their reliable distinguishability (with unit probability) requires a finite spatial domain. Two classical states (functions) can be reliably distinguished by their values at a single suitably chosen point.

The time interval T required for a reliable distinguishability of the states, i.e. the time of secure storage of the secrete bit, is determined by the spectrum bandwidth $\Delta|\mathbf{k}| \approx \Delta\omega/c$ of the photons used in the protocol and is estimated as $T \approx 1/\Delta\omega$. Note that although there are no any fundamental constraints on making the photon bandwidth arbitrarily small, this problem is technically very difficult.

5 Conclusions

We conclude with the following remark. The possibility of the state identification with the unit probability during time interval T depends on the existence for a particular type of particles of the states with finite spatial support. For the photons only the states with the exponentially localized energy and detection rate are known at present [18]. The latter formally means that the correct identification with unit probability is only possible for an infinite time interval. This consideration is not too restrictive fro the protocol since the time interval can be chosen to be sufficiently long to ensure the distinguishability probability exponentially close to unit for two orthogonal states.

The experimental realization is rather simple (at least in principle). It is sufficient to have N broadband sources. The term "broad band" here means that when turned on these sources produce the states localized in space and time, that is at the time moment t_0 one can prepare the signals with wide frequency spectrum. Before being allowed in the communication channel, these states should pass the narrow-band filters and attenuators to reach the one-photon level. Passage through the narrow-band filter requires either long time or large space. The detection is performed by the narrow-band detectors.

This work was supported by the Russian Foundation for Basic Research (project No 99-02-18127), grant No 02.04.5.2.40.T.50 within the framework of the Program "Advanced devices and technologies in micro- and nanoelectronics" and by the Program "Physics of quantum and wave processes" (subprogram "Quantum computing").

References

[1] C.H.Bennett, G.Brassard, *Proceedings of the International Conference on Computers, Systems and Signal Processing*, (IEEE, New York, 1984, p.175.

[2] G.Brassard, C.Crépeau, in *Advances in Cryptology: Proceedings of Crypto'90, Lecture Notes in Computer Science*, (Springer-Verlag, Berlin), v.537 (1991) p.49.

[3] G.Brassard, C.Crépeau, R.Jozsa, D.Langlois, in *Proceedings of 34th Annual IEEE Symposium Computer Society press, Los Alamitos, California*, (1993) p.362.

[4] M.Ardehali, quant-ph/9603019.

[5] H.-K.Lo, H.F.Chau, Phys. Rev. Lett., **78**, 3410 (1997).

[6] D.Mayers, Phys. Rev. Lett., **78**, 3414 (1997).

[7] A.Kent, quant-ph/9810068, Phys. Rev. Lett., **83**, 1447 (1999).

[8] A.Kent, quant-ph/9906103.

[9] W.K.Wootters, W.H.Zurek, Nature, **299**, 802 (1982).

[10] C.H.Bennett, Phys. Rev. Lett., **68**, 3121 (1992).

[11] L.Goldenberg, L.Vaidman, Phys. Rev. Lett., **75**, 1239 (1995).

[12] N.N.Bogolubov, D.V.Shirkov, *Introduction to the theory of quantum fields.*, Moscow, "Nauka", 1973.

[13] A.S.Holevo, *Probabilistic and Statistical aspects of the quantum theory*, Moscow, "Nauka", 1980.

[14] N.N.Bogolubov, A.A.Logunov, I.T.Todorov, *Foundations of the axiomatic approach to the quantum field theory*, Moscow, "Nauka", 1969.

[15] V.S.Vladimirov, *Equations of mathematical physics*, Moscow, "Nauka", 1971.

[16] Tal Mor, quant-ph/9906073.

[17] S.N.Molotkov and S.S.Nazin, ZhETF Letters,, **70**, 53 (1999) [JETP Lett., **70**, 54 (1999)].

[18] I.Bialynicki-Birula, Phys. Rev. Lett., **80**, 5247 (1998).